Claims

[c1] A method for securing a portable security module for use with a decoding element, the portable security module and the decoding element allowing to descramble scrambled audiovisual information, the method comprising :

processing at the portable security module Entitlement Control Messages (ECMs) received at the portable security module to allow the descrambling of the scrambled audiovisual information;

the method being characterized in that it further comprises :

analyzing (402) at the portable security module a sequence of ECMs, the sequence of ECMs comprising a new ECM and a previous ECM received at a previous time, the ECMs of the sequence being received at the portable security module at distinct times, the analyzing being performed at the receiving of the new ECM;

incrementing at the analyzing an error register upon a determined result of the analyzing (403);

applying a penalty to the portable security module depending on a value of the error register by introducing a dead time at the processing so as to slow down the processing (404).

[c2] The method according to claim 1, wherein the ECMs are replaced with Entitlement Management Messages (EMMs).

[c3] The method according to claim 1, wherein :

the dead time has a duration that depends on a value of the error register (404).

[c4] The method according to any one of claims 1 or 3, wherein

the duration of the dead time is shorter than a maximum time value;

the maximum time value is high enough to prevent the portable security module (31) from processing more than one ECM during a single cryptoperiod.

[c5] The method according to any one of claims 1, or 3 to 4, wherein :

each ECM (54_n, 54_{n+1}) comprises a channel identifier (51_n, 51_{n+1}), the channel identifier being associated to a determined channel;

the analyzing of the sequence of ECMs comprises comparing the channel identifier 51_{n+1} of the new ECM 54_{n+1} and the channel identifier 51_n of the previous ECM 54_n.

[c6] The method according to any one of claims 1, or 3 to 4, wherein :

each ECM (54_n, 54_{n+1}) comprises a first encrypted Control Word (52_n, 52_{n+1}) and a second encrypted Control Word (53_n, 53_{n+1});

the first Control Word allows to descramble the scrambled audiovisual information during a first cryptoperiod;

the second Control Word allows to descramble the scrambled audiovisual information during a second cryptoperiod distinct from the first cryptoperiod;

the analyzing of the sequence of ECMs comprises comparing a second Control Word 53_n of the previous ECM 54_n to a first Control Word 52_n of the new ECM 54_{n+1}.

[c7] The method according to any one of claims 1, or 3 to 4, wherein :

the analyzing of the sequence of ECMs comprises comparing a determined content of a first ECM of the sequence of ECMs to a second determined content of a second ECM of the sequence of ECMs.

[c8] The method according to any one of claims 1, or 3 to 7, further comprising :

introducing upon a reset a reset dead time at each processing of the ECMs, wherein:

the reset dead time has a duration that depends on a number of ECMs received at the portable security module after the reset, the duration being equal to a first reset time value at a first processing immediately following the reset;

the first reset time value is smaller than the maximum time value.

[c9] The method according to any one of claims 1, or 3 to 8, further comprising :

evaluating the nature of a further reset according to an intermediate group of intermediate ECMs, the intermediate group comprising the ECMs received after a previous reset preceding the further reset.

[c10] The method according to claim 9, further comprising :

counting the number of the intermediate ECMs (72);

comparing the number of the intermediate ECMs to a reset threshold number (73), wherein a result of the comparing allows to evaluate the nature of the further reset;

incrementing upon the further reset a reset error register (79) if the further reset is evaluated as suspicious;

blocking the portable security module (711) if the reset error register has a value that is higher than a reset errors threshold.

[c11] A portable security module (31) for use with a decoding element, wherein the portable security module and the decoding element allow to descramble scrambled audiovisual information, the portable security module comprising:

receiving means to receive Entitlement Control Messages (ECMs);

processing means (32) to process an ECM received at the portable security module so as to allow the descrambling of the scrambled audiovisual information;

the portable security module being characterized in that it further comprises :

a command message memory (36) into which a previous ECM (ECM_n) received at a previous time may be stored;

analyzing means (35) to analyze a sequence of ECMs, the sequence of ECMs comprising a new ECM and the previous ECM, the ECMs of the sequence being received at the portable security module at distinct times, and the analyzing being performed at each receiving of a new ECM (ECM_{n+1});

comparing means to compare the new ECM and the previous ECM of the sequence of ECMs;

an error register (37);

incrementing means to increment the error register depending on a result of the comparing;

delaying means to introduce a dead time at each processing so as to slow down the processing.

[c12] The portable security module (31) according to claim 11, wherein :

the delaying means also allow upon a reset to introduce a reset dead time at each processing following the reset;

the reset dead time has a duration that depends on a number of processing following the reset, the duration being equal to a first reset time value at a first processing immediately following the reset.

[c13] The portable security module (31) according to any one of claims 11 to 12, further comprising :

a count register allowing to store a number of intermediate ECMs, the intermediate ECMs being received at the portable security module after a previous reset;

a flag, the flag having a value that depends on a result of a comparing of the count register to a reset threshold number;

a reset error register that is incremented depending on the value of the flag upon a further reset;

blocking means to block the portable security module according to a value of the reset error register.

[c14] The portable security module according to any one of claim 11 to 13, wherein the ECMs are replaced by Entitlement Management Messages (EMMs).

[c15] A computer program for use within a portable security module, wherein the computer program implements the method according to any one of claims 1 to 10.

[c16] A method for securing a portable security module comprising downloading a software that allows to implement a method according to any one of claims 1 to 10, wherein the downloading comprises receiving at the portable security module at least one configuration message from the decoding element.